AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

845 ARITAS ROAD SW,
ALBUQUERQUE, NM 87105

Case No. 25-MR-380

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A (incorporated by reference).

located in the _____ District of New Mexico, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B (incorporated by reference).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1201	Kidnapping
18 U.S.C. § 1203	Hostage Taking

The application is based on these facts:

Please see the attached affidavit of FBI Special Ageny Bryce Oleski, which is incorporated by reference and has been reviewed by AUSA Lou Mattei.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Bryce Oleski
Applicant's signature

Bryce Oleski, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephonically sworn and electronically signed *(specify reliable electronic means)*.

Date: March 2, 2025

Laura Fashing
Judge's signature

City and state: Albuquerque, New Mexico

Laura Fashing, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF: 845 ARITAS ROAD SW, ALBUQUERQUE, NM 87105.	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Bryce Oleski, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 845 Aritas Road SW, Albuquerque, NM 87105, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since 2017. I have investigated white collar crime, cyber crime, and violent crime specifically violations which involve an imminent threat to life. I have been assigned to the Albuquerque Division since 2022, where I have conducted investigations into kidnapping for ransom and imminent violent threats involving an interstate nexus. My duties include, but are not limited to, the investigation and enforcement of criminal violations related to kidnapping for ransom and imminent threats made via interstate communication.

3. I make this affidavit based upon my own personal knowledge, which is substantially derived from my participation in the investigation, as well as that of fellow agents and officers who have participated in the investigation. This affidavit is intended to show only

that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

FEDERAL CHARGES RELEVANT TO THIS INVESTIGATION

4. I believe there is probable cause that unknown subjects have committed, are committing, and will continue to commit offenses involving violations of, *inter alia*:

a. 18 U.S.C. § 1201, that being Kidnapping; and

b. 18 U.S.C. § 1203, that being Hostage Taking.

ELECTRONIC MEDIA AND FORENSIC ANALYSIS

5. As described in Attachment B, this application seeks permission to search for evidence and records that might be found on the PREMISES, in whatever form they are found. Much of the evidence and records described in the paragraphs below, and in Attachment B, can also be produced and/or stored on electronic media. For this reason, I submit that if a computer, digital medium, or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer, digital medium, or storage medium. Thus, the warrant applied for would authorize the seizure of electronic media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

6. *Necessity of seizing or copying entire electronic media.* In most cases, a thorough search of a premises for information that might be stored on electronic media often requires the seizure of the physical electronic media and later off-site review consistent with the warrant. In lieu of removing electronic media from the premises, it is sometimes possible to make an image copy of electronic media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the

electronic media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Electronic media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the electronic media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of electronic media formats that may require off-site reviewing with specialized forensic tools.

7. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying electronic media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the computer or entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

8. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints

that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will

unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

PROBABLE CAUSE

I. Background about Human Smuggling Organizations (HSOs)

9. Based on my training and experience, I know it is common for human smuggling organizations (HSOs) to engage in kidnapping and hostage-taking. HSOs typically smuggle

undocumented individuals from foreign countries into the United States in exchange for an agreed-upon fee. After successfully transporting those individuals into the United States, HSO members and their associates will contact family members of the person who was smuggled and demand additional payment before releasing the person and/or to ensure the person is not harmed. Oftentimes, these victims are held in HSO-run stash houses against their will and by force (to include by threat of violence and the use and display of weapons, such as firearms) until additional payment is made. I believe the facts described below include several features of such a scheme.

10. I also know that it is common for HSOs to engage in other forms of criminal activity, to include drug trafficking, firearms trafficking, and money laundering. This is particularly true where the HSO is affiliated with a major transnational criminal organization, such as a Mexican drug cartel. For this reason, it is common to find illegal controlled substances and firearms in HSO stash locations where kidnapping and hostage-taking victims are being held.

II. Report of Ransom Demand

11. On March 1, 2025, a COMPLAINANT contacted the FBI and reported the kidnapping of VICTIM (the COMPLAINANT's spouse). COMPLAINANT received a phone call from phone number 505-524-6196 and was advised by UNIDENTIFIED SUBJECTS to pay a ransom of 90,000 quetzales (Guatemalan currency)[1] to ensure the VICTIM's safety. The UNIDENTIFIED SUBJECTS told COMPLAINANT that the VICTIM would be turned over to the Zeta Cartel (also known as Los Zetas)[2] if payment was not made by March 4, 2025. The

[1] This is roughly $11,600 in U.S. currency.

[2] According to the U.S. State Department, Los Zetas, or Cártel del Noreste (CDN), is a transnational organization based in northeastern Mexico involved in drug trafficking, kidnapping, extortion, human

COMPLAINANT reported that four UNIDENTIFIED SUBJECTS participated in this call. One had a Guatemalan accent, one a Mexican accent, and one spoke poor Spanish but better English.

12. The COMPLAINANT stated the VICTIM had entered into the United States in January of 2025. The VICTIM was living and working in Albuquerque, New Mexico, and the VICTIM had spoken with the COMPLAINANT daily until approximately February 23, 2025. During these calls, the VICTIM used Guatemalan phone number 3399-3889.

13. On March 1, 2025, the COMPLAINANT received audio and video recordings from various phone numbers, to include the same 505-524-6196 number noted above. Initially, a video was sent of the VICTIM stating his/her name, the date, and that the VICTIM was being held by his/her abductors in Albuquerque, New Mexico. Based on my training and experience, this video was consistent with a "proof of life" video that is commonly sent in hostage-taking events.

14. Later on March 1, 2025, the COMPLAINANT received an audio recording from the same 505-524-6196 number noted above. The COMPLAINANT also received a video file from Guatemalan phone number 4620-8504. These communications instructed the COMPLAINANT to take a photo of the demanded ransom money and send it to the Guatemalan phone number. When that was complete, the COMPLAINANT would be sent a Guatemalan bank account number for deposit of the money. The UNIDENTIFIED SUBJECTS also specified a demand for the COMPLAINANT to have 20,000 quetzales[3] by the end of March 1, 2025, or the

---

smuggling, and other illicit activities. CDN uses violence to exert its criminal control, including attacks against government officials in Mexico. *See* https://www.state.gov/designation-of-international-cartels/.

[3] Around $2,500 in U.S. currency.

VICTIM would be turned over to "the mafia." The COMPLAINANT believed that if the VICTIM was turned over to "the mafia," they would be harmed due to non-payment of the ransom.

15. The FBI is in possession of copies of these files and has confirmed the substance of the content described above.

III. Location of the Cell Phone Using Phone Number 505-524-6196

16. As noted above, the cell phone using phone number 505-524-6196 made at least two communications related to the hostage-taking scheme described above.

17. Pursuant to an exigent request to AT&T Global Legal Demand Center, this cell phone was identified as a prepaid account subscribed to a David Gonzalez, 681 Emerald Avenue, El Cajon, CA 92020, with email address david121@gmail.com.

18. A location ping on March 1, 2025, at 21:13:09 GMT showed the approximate location of this phone to be near GPS coordinates 35.041800, -106.672214, or approximately 2015 La Vega Dr. SW, Albuquerque, NM 87105, with an uncertainty radius of 272 meters.

19. Later on March 1, 2025, agents obtained court authorization to use a cell-site simulator device to obtain the precise location of this cell phone. Based on my training and experience, and that of other agents involved in this investigation, I know that such a device can locate a cell phone with enough precision to determine that it is present within a particular residence.

20. At approximately 11 p.m. on March 1, 2025, agents deployed the cell-site simulator device in the vicinity of the GPS coordinates described above. By approximately 11:54 p.m., agents determined that the cell phone using phone number 505-524-6196 was located inside the PREMISES.

21. Based on these facts, there is probable cause to believe the PREMISES will contain evidence related to violations of 18 U.S.C. § 1201, that being Kidnapping, and 18 U.S.C. § 1203, that being Hostage Taking.

CONCLUSION

22. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

Bryce Oleski

BRYCE OLESKI
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION

Telephonically sworn and electronically signed on March 2, 2025.

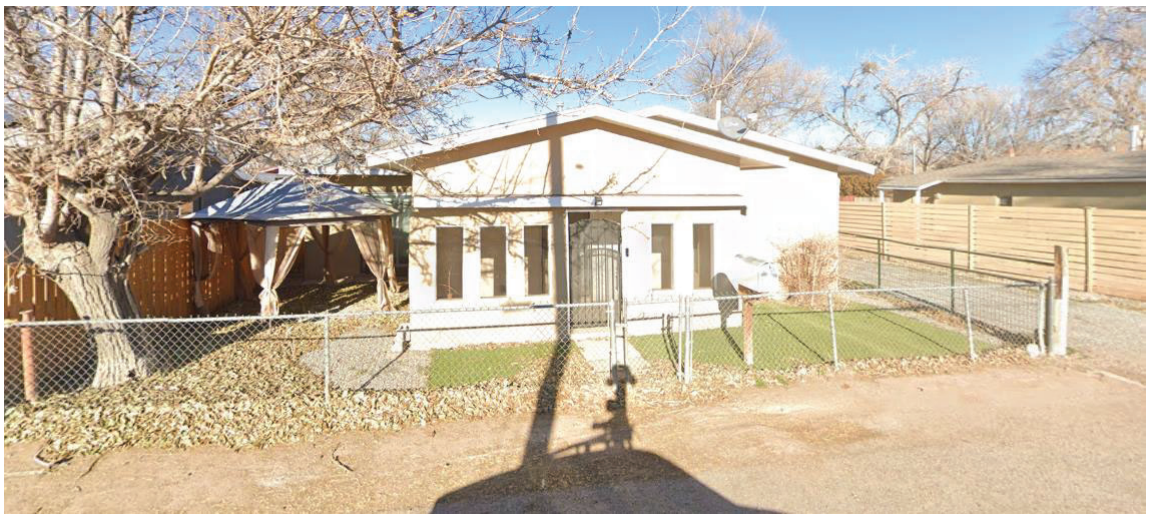
Laura Fashing

LAURA FASHING
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 845 Aritas Road SW, Albuquerque, NM 87105, hereinafter "PREMISES," further described as a white single-story house surrounded by a chain-link fence. A photograph of the exterior of the PREMISES is included below. Note that this image was obtained through Google Maps and may not reflect the current appearance of the PREMISES.



The search of the above PREMISES shall include the search of the entire residence, all attached and unattached garages and storage areas/containers (including mailboxes and trash cans) on the PREMISES, and all persons located on the PREMISES in or on which the items to be seized could be concealed. The search shall also include all vehicles parked at, or in front of, the PREMISES that have an apparent connection to the PREMISES and/or the SUBJECTS. Connection to the vehicle may be established by evidence that anyone residing at the PREMISES and/or the SUBJECTS own, operate, and/or have access to any vehicle parked at or in front of the PREMISES. Evidence includes prior law enforcement observation, vehicle registration, subject admission, or possession of an ignition key.

ATTACHMENT B

Property to be seized

All records, information, and evidence relating to violations of 18 U.S.C. § 1201, that being Kidnapping, and 18 U.S.C. § 1203, that being Hostage Taking, those violations involving unknown suspects and occurring after February 23, 2025, including:

1. Controlled substances, packaging, and paraphernalia related to controlled substances.
2. Weapons, including firearms and ammunition, handguns, rifles, shotguns, and automatic weapons.
3. Large amounts of currency, financial instruments, precious metals, jewelry and other items of value.
4. Any and all ledgers, lists, records, or notes containing the individual names of persons held at the PREMISES or by any person reasonably associated with the PREMISES; telephone numbers and addresses of these individuals; and any corresponding records of accounts receivable, money paid or received, or cash received in association with the holding or transportation of these individuals.
5. Telephone and address books or notes containing telephone numbers and addresses of co-conspirators.
6. Messages, notes, correspondence, and communications between kidnapping and hostage-taking associates, and to other victims and their relatives.
7. Indications of ownership or control of the PREMISES and other premises used in unlawful kidnapping or hostage-taking activity, including but not limited to, utility bills, cancelled checks, or envelopes and deeds or leases.

8. Indications of ownership or control over any vehicles located at the PREMISES, including but not limited to, titles, registrations, gas receipts, repair bills and keys belonging to that vehicle.
9. Records, receipts, bank statements and records, money drafts, letters of credit, money orders and cashier's checks received, passbooks, bank checks, safe deposit box keys, vault keys, safes and other items evidencing the obtaining, secreting and/or concealment, and or expenditures of money.
10. Photographs or videos of the kidnappers and hostage-takers, and any co-conspirators.
11. Other financial records, which may include airline ticket receipts, credit card receipts, rental car receipts and luggage tags reflecting points of travel.
12. Digital video surveillance systems, including the associated storage media.
13. Any and all computers, digital media, and storage media that reasonably appear to contain some or all of the records, information, and/or evidence described in Attachment B.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer, digital media, or storage media; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "digital media" includes personal digital assistants (PDAs), smartphones, tablets, BlackBerry devices, iPhones, iPads, digital cameras, and cellular telephones.

The term "storage media" includes any physical object upon which electronic data can be recorded, such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media or digital medium.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, smartphones, tablets, server computers, and network hardware.

This warrant authorizes a review of all electronic media seized pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The warrant also authorizes a review of all electronic media for evidence of who used, owned, or controlled the electronic media at the time the things described in this warrant were created, edited, or deleted. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual who is found at the PREMISES and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.